Some Open Issues Concerning the Semantics of ODRL 2.2

Piero Andrea Bonatti[1], Nicoletta Fornara[2,*] and Andreas Harth[3]

[1]University of Naples "Federico II", Napoli, Italy
[2]Università della Svizzera italiana, Lugano, Switzerland
[3]Friedrich-Alexander-Universität Erlangen-Nürnberg & Fraunhofer Institute for Integrated Circuits IIS, Nuremberg, Germany

Abstract

The Open Digital Rights Language (ODRL 2.2) is a popular candidate for a policy language applied in scenarios where parties exchange data, such as in data spaces. The W3C specifications around ODRL 2.2 are written in prose and lack a rigorous formal semantics. Based on our attempts at proposing a formal semantics for ODRL 2.2, we have identified several shortcomings in the current W3C specifications. We believe that an upcoming version of ODRL should address these issues.

1. Introduction

The realization of open and distributed ecosystems in which organizations, individuals, and digital companions can exchange data or resources is becoming increasingly important, as shown by the studies of various W3C Community Groups and data space initiatives supported by the European Commission[1]. Prerequisites for the realization of such systems are: (i) the sovereignty of participants over their resources, i.e., the ability to define rules for accessing and using these resources; (ii) the possibility of establishing interactions based on agreements and policies; (iii) the ability to verify that interactions comply with stipulated agreements and policies, as well as with applicable legislation. Central to the construction of such systems is a policy language capable of expressing permissions, prohibitions, and obligations governing the actions that can be performed on digital resources.

The Open Digital Rights Language (ODRL) is a policy language that can be applied to a broad variety of scenarios. Originally designed for Digital Rights Management (DRM), ODRL is now being used to express manifold contracts and policies, such as data licensing [1], privacy policies [2], and access control policies [3].

It is essential that the party that states a policy and the party that must comply with the policy share a common understanding of the policy's meaning. In addition, as many scenarios require the processing of large numbers of policies, the various tasks involving policies should be automated and implemented in software. However, meeting the above natural desiderata is challenging as the two official ODRL 2.2 documents concerning the Information Model [4] and the Vocabulary [5] define the meaning of policies in natural language.

The W3C ODRL Community Group is aware of the lack of a formal semantics for ODRL and has published a draft report on ODRL semantics [6]. In [7], we proposed a declarative semantics for ODRL 2.2 that covers a subset of the language that includes only ODRL's main features: permissions, prohibitions, duties, refinements, and constraints. Thanks to this systematic work, we were able to point out "gray areas" in ODRL's informal semantics, as well as lack of expressiveness that we discuss in the remainder of the paper. We will illustrate these issues using concrete examples that we may encounter when using online services and sharing digital assets.

W3C Workshop on the Future of ODRL 20 & 21 July 2026 London, UK.
*Corresponding author.
pab@unina.it (P. A. Bonatti); nicoletta.fornara@usi.ch (N. Fornara); andreas.harth@fau.de (A. Harth)
https://www.linkedin.com/in/piero-bonatti-819b49/ (P. A. Bonatti); www.linkedin.com/in/nicoletta-fornara-0384397 (N. Fornara); https://www.linkedin.com/in/aharth/ (A. Harth)

[1]https://digital-strategy.ec.europa.eu/en/policies/data-spaces

2. Issues

The following shortcomings of ODRL 2.2 are based on the specifications written in natural language available in the ODRL Information Model 2.2 [4] and in the ODRL Vocabulary & Expression 2.2 [5].

2.1. Compliance with Permission

The intuitive meaning of a permission, as defined in [4], is as follows: "A Permission **allows** an action, with all refinements **satisfied**, to be **exercised** on an Asset if all constraints are **satisfied** and if all duties are **fulfilled**.".

Definition 1. (Compliance with a permission with duties) In [7, Section 3.5], a formal definition is provided of the conditions that must hold for an action a to be compliant with an permission π in state S. Those conditions (which relate to the various properties of a permission, including its duties, and the properties of action a) are reported here using an informal notation (see [7] for the full formal details):

1. All of the rule's **constraints** are **satisfied** by the action a;
2. All of the rule's **duties** are **fulfilled** by the action a;
3. Action a **belongs** to the permitted class of actions;
4. The action's target **equals** the target of the Permission or it is contained in the collection of objects specified as the target of the Permission;
5. When the assignee of the permission is specified, the action's party **equals** the assignee of the Permission or it is contained in the collection of parties specified as assignee of the Permission;
6. All the refinements (if any) of the regulated action, target, and assignee are **satisfied** by action a, its target and its party (respectively).

Definition 2. (Compliance with a duty inside a permission) Section 3.6 of [7] formally defines the conditions which must hold for a duty ω (inside a Permission) to be **fulfilled** by an action $a2$ in a state S. Those conditions are reported here using an informal notation:

1. Every **constraint** of the duty is **satisfied** by the action a that is regulated by the Permission (roughly speaking, a is the action that – in order to be exercised in compliance with the permission – needs a_2 to be exercised to fulfill the duty);
2. Action $a2$ belongs to the class of actions required by the duty;
3. Action $a2$ is performed **before** action a;
4. Action $a2$ satisfies all the refinements (when they are specified) related to the action(s) required by the duty;
5. If a target object of the duty is specified, then the assets involved in action $a2$ are **exactly** those specified in the target of the duty and its refinements;
6. If an assignee party of the duty is specified, then the parties that exercise action $a2$ are **exactly** those specified in the assignee of the duty and its refinements.

Issue 1: Different semantics for the **fulfillment** of duties are possible. In Definition 2, the action must be exercised jointly by all the specified assignees (as in: *the contract shall be approved by all assignees*). Alternatively, one might require that the action be exercised by *any* of the specified assignees (as in: *the payment shall be made by any of the assignees*), or that each assignee should independently fulfill the duty (e.g. *all assignees shall register*). Each of these three semantics is useful in different use cases. Unfortunately, ODRL does not clarify which of the above semantics is the intended one, and it is not expressive enough to select the desired semantics, based on the use case.

Issue 2: Duty constraints may be fulfilled by different actions. Def. 2, states that the duty's constraints are satisfied by the Permission's action a (as in: *a ticket has to be paid to enter the museum on Sunday*,

where *on Sunday* refers to *entering* the museum). Alternatively, constraints might have to be satisfied by action $a2$ (as in: *a ticket has to be paid on Sunday to enter the museum*; in this case, the *payment* must be made on Sunday – say, because the ticket office is only open on that day – then the museum can be entered anytime after the payment). ODRL must clarify which semantics if the intended one.

Issue 3: Different notions of compliance are possible, for permissions with duties. In Definition 1, a single duty fulfillment by an action $a2$ suffices to permit any number of actions. This can be useful to say, for example, that *after registering to a web site (once and for all), a user may access all the contents of the web site*. In other use cases, one may need to say that *each* execution of the action regulated by the permission requires a different fulfillment of the duty; this would be useful to specify *pay-per-view* policies.

Issue 4: The ODRL Information Model specification states that a duty is "an agreed Action that MUST be exercised (as a pre-condition to be granted the Permission)" and that "the duty property asserts a pre-condition between the Permission and the Duty". Accordingly, fulfillment has been formalized in Definition 2 by requiring that the duty is fulfilled before exercising the permitted action. However, this notion of fulfillment cannot model duties that occur in the future, as in the norm: "*personal data can be collected but it must be deleted within one month*". A possible alternative interpretation of the specification is that the assignee(s) must *agree* to fulfill the duty before exercising the permission (the duty may be fulfilled later); however, such agreement is not formalized in the specification, therefore also this alternative interpretation needs clarifications.

Issue 5: Sections 2.6.3 and 2.6.4 of ODRL's Information Model [4] state that "A duty is fulfilled *if all constraints are satisfied* and if its action, with all refinements satisfied, has been exercised". The above definitions formalize this statement. There exists, however, another way of intending the role of constraints in duties; it could be stipulated that the duty is active – and its action shall be exercised – *only if the constraints are satisfied* (otherwise, the duty can essentially be ignored). Some of the examples in the ODRL Information Model are apparently using the latter meaning rather than the specified semantics (cf. Example 22).

2.2. Complying With a Policy

An ODRL policy Π may contain one or more rules (permissions, prohibitions, and duties, possibly of different types) plus several properties for specifying namespaces and profiles, and a property "conflict" with possible values "perm" (permissions have precedence), "prohibit" (prohibitions have precedence), "invalid" (conflicts generate an error); the latter is the default value.

Issue 6: ODRL cannot express gap resolution strategies, where "gap" means that an action is neither permitted nor prohibited. There are at least two standard approaches to resolving policy gaps in data security: *open* and *closed* default policies, that permit and deny the action, respectively. In the absence of references to gap resolution in ODRL's specification, we will (temporarily) adopt the most conservative approach, namely, the closed default policy. The reader may easily verify that prohibitions still make sense when they partially overlap permissions, unless the conflict resolution strategy is "perm"; in that case, prohibitions are irrelevant and useless.

Definition 3. Consider a policy Π with permissions $\pi_1, \ldots, \pi_p$, prohibitions $\rho_1, \ldots, \rho_d$, obligations $\omega_1, \ldots, \omega_o$, and conflict value s (for "strategy"). For a state S we say that: S *complies* with Π, according to the closed gap resolution, if and only if all of the following conditions hold:

1. for all active obligations there exists an action a_i in S that fulfills the obligation;
2. for all actions $a \in S$, at least **one of the** following two conditions holds:

a) a is either a fulfilling action a_i for an obligation ω_i of Π, or a fulfilling action for the duty of some permission π_i;
b) there exists a permission π_i such that a complies with π_i in S, and either $s =$"perm" or a complies with all the prohibitions $\rho_1, \ldots, \rho_d$ in S.

In other words, a trace complies with Π if all the obligations are fulfilled, and all actions are either required or permitted. Point 2b deals with the latter; the existence of an applicable permission is enough if $s =$"perm" (because in this case the permission overrides any infringed prohibition), while for the other strategies s, a shall comply with all prohibitions. To understand point 2a, first note a crucial point:

Issue 7: The fulfilling actions of obligations and duties may have to be authorized, too, but they may fall outside the scope of the policy Π, in general. For example, a content provider may state in Π that an mp3 can be played only after fulfilling the duty of paying €2 online, and this action is either permitted or denied by the policy Π' of another company (the bank). This observation reveals a set of open issues: ODRL provides no means to define the *scope* of a policy (i.e. which actions must comply with which policy), nor whether there are actions that are not subject to any policy and may be freely exercised. Moreover there is no guideline about the interplay of different policies, of which the provider + bank example is just one particular instance; in more complex examples, Π and Π' may "overlap" and conflicts may have to be resolved.

In [7] we tackled the above above issue with a temporary solution, i.e. by stipulating (through point 2a) that fulfilling actions are implicitly compliant *with the policy that requests those actions*. Thus, in the above example, the €2 payment complies with the policy Π of the content provider (which "requests" that action as a duty when the file is played), although it may infringe the policy Π' of the bank. A cleaner solution needs ODRL to be extended with a notion of *policy scope*.

References

[1] V. Rodríguez-Doncel, S. Villata, A. Gómez-Pérez, A dataset of RDF licenses, in: Legal Knowledge and Information Systems - JURIX 2014, Krakow, Poland, 10-12 December 2014, volume 271 of *Frontiers in Artificial Intelligence and Applications*, IOS Press, 2014, pp. 187–188. doi:10.3233/978-1-61499-468-8-187.

[2] H. J. Pandit, B. Esteves, G. P. Krog, P. Ryan, D. Golpayegani, J. Flake, Data privacy vocabulary (DPV) - version 2.0, in: The Semantic Web - ISWC 2024, Proceedings, Part III, volume 15233 of *Lecture Notes in Computer Science*, Springer, 2024, pp. 171–193. doi:10.1007/978-3-031-77847-6_10.

[3] B. Esteves, V. Rodríguez-Doncel, H. J. Pandit, N. Mondada, P. McBennett, Using the ODRL Profile for Access Control for Solid Pod Resource Governance, in: The Semantic Web: ESWC 2022 Satellite Events - Hersonissos, Crete, Greece, May 29 - June 2, 2022, Proceedings, volume 13384 of *Lecture Notes in Computer Science*, Springer, 2022, pp. 16–20. doi:10.1007/978-3-031-11609-4_3.

[4] R. Iannella, S. Villata, ODRL Information Model 2.2, Recommendation, W3C, 2018. https://www.w3.org/TR/2018/REC-odrl-model-20180215/. Latest version available at https://www.w3.org/TR/odrl-model/.

[5] R. Iannella, M. Steidl, S. Myles, V. Rodríguez-Doncel, ODRL Vocabulary & Expression 2.2, Recommendation, W3C, 2018. https://www.w3.org/TR/2018/REC-odrl-vocab-20180215/. Latest version available at https://www.w3.org/TR/odrl-vocab/.

[6] N. Fornara, V. Rodríguez-Doncel, B. Esteves, S. Steyskal, B. W. Smith, Y. Sellami, A. C. Arriaga, ODRL Formal Semantics, Draft Community Group Report, W3C, 2026. https://w3c.github.io/odrl/formal-semantics/.

[7] P. A. Bonatti, N. Fornara, A. Harth, Towards a formal semantics of the open digital rights language (ODRL 2.2), in: M. Sabou, et al. (Eds.), Joint Proceedings of the ESWC 2025 Workshops and Tutorials co-located with 22nd Extended Semantic Web Conference (ESWC 2025), Portorož, Slovenia, June 1-2, 2025, volume 3977 of *CEUR Workshop Proceedings*, CEUR-WS.org, 2025. URL: https://ceur-ws.org/Vol-3977/OPAL2025-4.pdf.